

(i) Every effort shall be made to limit production of classified information to an *in camera*, *ex parte* review by the court to determine the relevance of the classified information in question.

(ii) Classified information shall not be introduced into evidence or otherwise disclosed at a proceeding without the prior approval of either the originating agency, the Attorney General, or the President.

(iii) Attendance at any proceeding where classified information is to be introduced or disclosed should be limited to the judge(s) as defined in Department Order 2620.6 and to those other persons whose duties require knowledge or possession of the classified information who have been determined to be trustworthy by the Department Security Officer.

(iv) All such proceedings shall be held in a court facility which can provide appropriate protection for the classified information as determined by the Department Security Officer.

(v) Dissemination and accountability controls shall be established for all classified information offered for identification or introduced into evidence at such proceedings.

(vi) All transcripts of such proceedings shall be appropriately marked to show the classified portions and placed under seal upon transcription.

(vii) All classified information including the appropriate portions of the transcript shall be handled and stored in a manner consistent with the provisions of this regulation.

(viii) At the conclusion of the proceeding, all classified information shall be returned to the Department or placed under seal by the court.

(ix) All classified notes, drafts, or any other documents generated during the course of the proceedings and containing classified information shall be retrieved by Department employees and immediately transferred to the Department for safeguarding and destruction as appropriate.

(x) All persons who become privy to classified information disclosed under the provisions of this section shall be fully advised as to the classification level of such information, all pertinent safeguarding and storage requirements,

and their liability in the event of unauthorized disclosure.

(xi) The Department Security Officer, in consultation with the agency originating classified case-related information and Government attorneys, may waive any of the security requirements identified in paragraph (g)(4)(iii)–(x) of this section, if it has been determined that such a waiver is in the interest of the national security.

(5) This paragraph shall apply to all litigation, including matters arising under the Freedom of Information Act, 5 U.S.C. 552, as amended.

**§ 17.97 Access by foreign nationals, foreign governments, international organizations, and immigrant aliens.**

(a) Classified information may be released to foreign nationals, foreign governments and international organizations only when authorized under the provisions of the National Disclosure Policy (NDP-1) issued by the Secretary of Defense.

(b) If it is in the interest of the national security, Secret and Confidential information may be released, on a limited basis, to immigrant aliens in the performance of official duties, provided that the Department Security Officer determines the individual is reliable and trustworthy in accordance with this subpart.

(c) Immigrant aliens may be granted a Limited Access Authorization to Top Secret information provided that the head of the Office, Board, Division of Bureau concerned makes a personal written request and determination to the Department Security Officer that such access is essential to meet Government requirements and that the Department Security Officer determines that the individual is reliable and trustworthy in accordance with this subpart.

**§ 17.98 Procedures for requesting a security clearance for a Department employee.**

Requests for determination of eligibility for a security clearance shall be in the form of a memorandum addressed from the head of the Office, Board, Division or Bureau concerned to the Department Security Officer. Exception to this requirement may be

## Department of Justice

## § 17.100

granted in accordance with the provisions of § 17.95(c). Two copies of the request shall be submitted. The memorandum shall contain the following items:

(a) *Degree of clearance requested.* National security clearances are categorized into three levels, namely, Top Secret, Secret, and Confidential. The categories of security clearances are related directly to the levels of National Security Information to which access is required.

(b) *Justification for requested clearance.* A person must have a need for access to the particular classified information or material sought in connection with his/her official duties or obligations. This need-to-know is the essence for any justification for a security clearance. The justification for a clearance does not have to be long or detailed; however, a strict need-to-know shall be established before consideration to grant a security clearance can be given.

(c) *Continuous evaluation of need-to-know.* A continuing review of the established need-to-know shall be conducted by the Security Programs Manager.

(d) *Request for administrative withdrawal.* The head of each Office, Board, Division or Bureau shall make provision to request the administrative withdrawal of a security clearance of persons for whom there is no foreseeable need for access to classified information or material in connection with the performance of their official duties; for example, termination of employment or change in position. Likewise, when a person no longer needs access to classified material bearing a particular security classification category, a request that the security clearance be adjusted to the classification category still required for the performance of his/her official duties and obligations shall be made by the Security Programs Manager of the Office, Board, Division or Bureau concerned. In both instances, such action resultant from these requests will be without prejudice to the person's eligibility for future security clearances.

### § 17.99 Other access situations.

When necessary in the interests of national security, the Attorney Gen-

eral or the Assistant Attorney General for Administration may authorize access by persons outside the Federal Government, other than those enumerated above, to classified information upon determining that (a) the recipient is trustworthy for the purpose of accomplishing a national security objective and (b) that the recipient can and will safeguard the information from unauthorized disclosure. The clearance procedures and provisions of Department Order 2620.6 shall be followed in such instances.

### § 17.100 Dissemination.

(a) *Policy.* Except as otherwise provided in section 102 of the National Security Act of 1947, 50 U.S.C. 403, and 17.96(f) of this regulation, classified information originating within the Department may not be disseminated outside any other agency to which it has been made available without the consent of the Department. Conversely, classified information originating in a department or agency other than the Department shall not be disseminated outside the Department without first obtaining the consent of the originating department or agency. Office, Board, Division and Bureau Security Programs Managers shall establish procedures consistent with this regulation for the dissemination of classified information. The originating official or Office, Board, Division or Bureau may prescribe specific restrictions on dissemination of classified information when necessary.

(b) *Restraint on reproduction.* No documents or materials or any portions thereof that contain Top Secret information shall be reproduced without the consent of the originator or higher authority. Any stated prohibition or markings on any classified document (regardless of classification) against reproduction shall be strictly observed. (See § 17.70.) The following measures apply to reproduction equipment and to the reproduction of classified information:

(1) Copying of documents containing classified information shall be minimized;

(2) Officials within each Office, Board, Division or Bureau shall be authorized by the Security Programs